

TECHNOLOGICAL DEVELOPMENS IN ELECTRONIC EVIDENCE IN CORRUPTION CASES

Hendra

Faculty of Law, Palembang University
hendrasaidi190@gmail.com

Hary Suharto

Faculty of Law, Palembang University
Harisuharto.hdw@gmail.com

Barhamudin

Faculty of Law, Palembang University
barhamudin@unpal.ac.id

Dewi Mulyati

Faculty of Law, Palembang University
Dewimulyati05.dm@gmail.com

Ali Dahwir

Faculty of Law, Palembang University
alidahwir@unpal.ac.id

Abstract

The development of information technology has had a significant impact on the evidentiary system in criminal law enforcement, particularly in corruption cases that are becoming increasingly complex and sophisticated. The use of electronic evidence has emerged as a crucial innovation in uncovering corruption offenses, which are often carried out through digital transactions, online communications, and electronic financial systems. This study aims to analyze the technological developments in the use of electronic evidence and its effectiveness in the evidentiary process of corruption cases. The research employs a normative juridical approach by examining statutory regulations such as Law No. 30 of 2002 concerning the Corruption Eradication Commission and Law No. 31 of 1999 in conjunction with Law No. 20 of 2001 concerning the Eradication of Corruption Crimes. The findings indicate that technological advancement has expanded the types and forms of evidence, including digital recordings, emails, electronic banking transaction data, and metadata, which are now legally recognized as valid evidence. However, the main challenges lie in ensuring the authenticity, validity, and integrity of electronic data, which require digital forensic expertise and more adaptive legal frameworks. Therefore, synergy among technological advancement, law enforcement capabilities, and regulatory reform is essential to optimize the use of electronic evidence in combating corruption in the digital era.

Keywords: *information technology, electronic evidence, corruption crime, proof, criminal law.*

1. INTRODUCTION

Criminal procedural law is a set of rules and procedures that governs the implementation of criminal law, specifically the manner in which formal criminal law is administered. According to Moeljatno, criminal procedural law constitutes a part of the overall legal system in a country that provides the fundamental principles and regulations determining the methods and procedures through which criminal sanctions for a criminal act

may be imposed when there is suspicion that an individual has committed such an offense (Moeljatno, 1995).

The purpose of criminal procedural law is to serve as a framework for upholding the truth. Law enforcement officials ranging from the police and prosecutors to judges must rely on established procedures throughout the investigative process, inquiry, prosecution, and adjudication of a defendant. These processes must be grounded in factual truth proven during the proceedings. Criminal procedural law, through the Indonesian Criminal Procedure Code (KUHAP), regulates the types of admissible evidence and the requirements for their validity, which are subsequently used by prosecutors to substantiate their charges in court.

Evidence refers to anything connected to an act that, through such evidentiary items, may be used to build proof that persuades the judge of the truth of a criminal offense allegedly committed by the defendant (Hari Sasongko & Lili Rosita, 2003). Under criminal procedural law, Article 184 paragraph (1) of KUHAP establishes five types of lawful evidence: witness testimony, expert testimony, documents, indications (*petunjuk*), and the defendant's statement. Criminal procedural law, as set out in KUHAP, regulates the types and validity requirements of admissible evidence, which are then employed by the public prosecutor to prove the charges during trial.

In addition to KUHAP, the provisions regarding evidence have expanded to include electronic evidence, which may be used in criminal proceedings based on special legislation. As society has evolved due to globalization, modernization, and advancements in information technology reflecting broader social changes—the enactment of Law No. 11 of 2008 on Electronic Information and Transactions (ITE), later strengthened by Law No. 19 of 2016, established that electronic information, electronic documents, and/or their printouts are recognized as an extension of lawful evidence in criminal procedure. The ITE Law is the first legislation in the field of Information Technology and Electronic Transactions, forming the foundational regulatory framework for the use of information technology and electronic transactions.

Electronic evidence is deemed admissible only in criminal acts regulated under the ITE Law and in specific offenses that explicitly recognize electronic evidence as lawful proof. As stipulated in Article 5 paragraph (1) of the ITE Law, electronic evidence consists of electronic information, electronic documents, and/or their printouts, which are valid legal evidence and constitute an extension of the types of lawful evidence recognized under KUHAP. Electronic evidence is therefore admissible only in offenses prescribed under the ITE Law and other particular offenses that expressly regulate the use of electronic evidence.

Corruption is a criminal offense whose regulation is governed through specific legislation. In a legal context, corruption refers to conduct in which an individual gains personal benefit at the expense of others, particularly when such acts are committed by public officials in violation of the law. However, from a broader perspective, corruption may also occur outside of governmental institutions, such as in the business sector, when laws are violated or unethical practices are carried out (Amalia Syauket & Dwi Seno Wijanarko, 2024). With regard to electronic evidence, the Law on the Eradication of Corruption Crimes provides specific provisions concerning the use of electronic evidence in corruption cases.

Advancements in technology and information systems have enabled perpetrators of corruption to transform their methods by exploiting information technology. Corruption offenses are increasingly conducted through online means, digital transactions, electronic communications, and electronic financial systems, positioning them within the broader category of cybercrime.

Various forms of corruption that have emerged in the digital era include:

1. Manipulation of Electronic Data

Corruption involving manipulation of electronic data often occurs within governmental or financial systems. Examples include altering budget data or illegally modifying tax payment systems.

2. Digital Procurement Fraud

Technology-based procurement systems are frequently targeted through collusion or bribery during online tender processes.

3. Misappropriation of Electronic Funds

The use of electronic payment platforms or digital wallets enables perpetrators to obscure the trail of misappropriated funds.

4. Sale of Confidential Data

Confidential governmental or corporate data can be traded on the digital black market (dark web), constituting a modern form of corruption.

Law No. 31 of 1999 on the Eradication of Corruption Crimes, as amended by Law No. 20 of 2001, outlines the types of lawful evidence admissible in corruption cases, including those derived from outside the provisions of Article 188 paragraph (2). Electronic evidence has become an essential innovation in efforts to uncover corruption offenses, which are often committed through digital transactions, online communications, and electronic financial systems.

Electronic evidence holds significant importance in criminal procedure. Its relevance lies in its ability to enhance the accuracy and reliability of proof, such as electronic data, audio recordings, or video recordings, thereby offering credible and trustworthy evidence in court proceedings.

Based on the background described above, the following research problems can be identified, How has technological development influenced the use of electronic evidence in corruption crimes, and what extent is the use of electronic evidence effective as a means of proof in criminal law.

The purpose of this research is to examine the development of technology in the use of electronic evidence and to assess the effectiveness of electronic evidence as a means of proof in criminal law. The practical benefit of this study is that its findings are expected to contribute valuable insights regarding the issues surrounding technological advancements in the use of electronic evidence in corruption crimes.

2. RESULTS AND DISCUSSION

2.1 Technological Developments in the Use of Electronic Evidence in Corruption

Crimes

Etymologically, the term *corruption* originates from the Latin word *corruption*, meaning decay or deterioration, and is also used to describe wrongful conditions or immoral acts (Elwi Danil, 2012). The words *corruptus* and *corruptio* literally signify rottenness, immorality, depravity, dishonesty, bribability, and deviation from integrity. Corruption is classified as an extraordinary crime (*extraordinary crime*) because it gravely undermines the foundations of societal and governmental systems and results in substantial losses to the state's economy.

Baharuddin Lopa asserts that corruption constitutes a criminal act involving bribery, manipulation, and other unlawful acts that harm state finances and the national economy, as well as the welfare and public interest.

According to Article 2 paragraph (1) of Law No. 31 of 1999 on the Eradication of Corruption Crimes, corruption is defined as an unlawful act that results in losses to state finances or the national economy. Furthermore, Article 26A of Law No. 20 of 2001 (amending Law No. 31 of 1999) explicitly recognizes electronic information and electronic documents as admissible evidence. The legal framework governing electronic evidence in Indonesia is grounded in several statutory instruments, including:

1. The Electronic Information and Transactions Law (Law No. 11 of 2008), which establishes the legal foundation for electronic evidence and acknowledges it as an extension of lawful evidence.
2. Constitutional Court Decision No. 20/PUU/XIV/2016, which affirms that recordings and other forms of electronic evidence possess evidentiary value in criminal proceedings, subject to the evidentiary standards of *bewijsvoering* (criminal evidentiary analysis).
3. Minister of Communication and Informatics Regulation No. 20 of 2016, which regulates procedures for processing and utilizing electronic evidence in cases pertaining to communication and informatics (Daniel David et.al., 2024).

Article 44 of the Electronic Information and Transactions Law (ITE Law) stipulates that evidence admissible in investigation, prosecution, and trial includes: evidence recognized under the applicable laws; and other evidence in the form of electronic information and/or electronic documents as defined in Article 1 points 1 and 4, and Article 5 paragraphs (1), (2), and (3).

Thus, in addition to evidence recognized under KUHAP, electronic information and/or electronic documents—including electronic mail—are admissible as lawful evidence. Law No. 20 of 2001 explicitly affirms that electronic evidence constitutes an expansion of the evidentiary category of *petunjuk* (indications).

Article 26A of Law No. 20 of 2001 provides that lawful evidence in the form of *petunjuk*, as referred to in Article 188 paragraph (2) of KUHAP, may also be obtained from:

- a. Other evidence consisting of information spoken, sent, received, or stored electronically by optical instruments or similar technologies; and
- b. Documents, including any recording or information that can be viewed, read, or heard, produced with or without a device, whether on paper, other physical media, or electronically recorded in the form of text, sound, images, maps, designs, photographs, symbols, numbers, or perforations that convey meaning.

The explanation of Article 26A clarifies that “stored electronically” includes data stored in microfilm, Compact Disk Read Only Memory (CD-ROM), or Write Once Read Many (WORM). The phrase “optical instruments or similar technologies” encompasses, but is not limited to, electronic data interchange (EDI), electronic mail, telegrams, telex, and facsimiles.

Further elaboration under Law No. 19 of 2016 (amending Law No. 11 of 2008) defines various forms of electronic information and electronic documents, including digitally stored, transmitted, or processed data, as well as the technological means used for such processes.

Based on Article 26A, electronic evidence forms an integral part of *petunjuk*. Electronic information and/or documents are recognized as lawful evidence in criminal procedure. Electronic evidence may therefore function as a substitute for documentary evidence, operate as an independent evidentiary category, and serve as an extension of *petunjuk*.

The Corruption Eradication Commission (KPK), as a state institution within the executive branch, has the mandate to prevent and eradicate corruption (Hasnawati, 2023). Pursuant to Article 12 paragraph (1) of Law No. 30 of 2002, KPK is authorized to conduct wiretapping and record communications involving individuals suspected of committing corruption.

Constitutional Court Decision No. 20/PUU-XIV/2016 categorizes wiretapping and recordings as electronic evidence obtained for the purposes of law enforcement upon the request of the police, prosecutors, or other legally authorized institutions under Article 31 paragraph (3) of the ITE Law.

KPK's authority to conduct wiretapping is grounded in Article 26A of Law No. 20 of 2001 and Article 12A of Law No. 30 of 2002. Wiretap results may be used as *petunjuk* in corruption cases. Although wiretap recordings alone do not constitute sufficient standalone evidence under criminal law, the information derived from them may serve as *petunjuk* in accordance with KUHAP. Thus, KPK remains bound by procedural requirements in carrying out investigations, inquiries, and prosecutions.

Wiretapping and related forms of electronic evidence have proven highly effective in uncovering corruption offenses and frequently lead to *Operasi Tangkap Tangan* (OTT), or arrest operations conducted in flagrante delicto. OTTs constitute one of KPK's most well-known enforcement methods and involve apprehending individuals caught in the act of committing corruption (Syaputra & Yudhistira, 2023).

In relation to OTTs, Article 12 of Law No. 30 of 2002 grants KPK the authority to conduct wiretapping and record all forms of electronic communications as part of its investigative powers. Wiretapping conducted by KPK is based on Article 12 paragraph (1), which reflects Article 6(c), granting KPK the authority to carry out investigations,

inquiries, and prosecutions of corruption offenses, including the authority to record communications of targeted individuals.

Interception is regulated under the Law on the Corruption Eradication Commission (KPK Law), which defines interception as the activity of listening to, recording, diverting, altering, obstructing, and/or documenting electronic information and/or electronic documents that are not publicly accessible, whether transmitted through wired or wireless communication networks such as electromagnetic emissions or radio frequencies.

There are six forms of interception, described as follows (Steve Jelly Walintukan et.al, 2022):

1. Wired Telephone Interception

This practice is carried out by installing devices on cable-based telephone networks and involves technologies that support the interception of information transmitted through fixed or wired telephone networks (Public Switched Telephone Network/PSTN).

2. Cellular Telephone Monitoring

This form of interception targets information transmitted through mobile or cellular communication networks.

3. Internet Monitoring

This form of communication interception involves capturing data in cyberspace during its transmission to its final destination (for example, data sent to a specific email address). This practice is omnipresent, as it can occur and be conducted anywhere within the digital environment.

4. Video Technology Monitoring

The most common form of video interception today is Closed-Circuit Television (CCTV), which is installed in specific locations to record any activity within its range. CCTV technology is capable of analyzing minute details of recorded subjects, such as biometric features of the face and even the cornea of the eye.

5. Global Positioning System (GPS) Location Monitoring

Location tracking involves the use of specialized software to visually record and report information captured within the network regarding the movement or position of a subject.

6. Communication Intrusion

This practice involves embedding software, such as certain types of malware, into a communication device to extract all information stored within it.

According to Article 5 paragraph (1) of Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), there are two categories that may be distinguished: first, electronic information and/or electronic documents, and second, printouts of electronic information and/or electronic documents. Electronic information and electronic documents constitute Electronic Evidence (Digital Evidence), whereas printouts of such information and documents constitute documentary evidence.

Article 5 paragraph (2) of Law No. 11 of 2008 on Electronic Information and Transactions stipulates that electronic information and/or electronic documents and/or their printouts constitute an extension of legally valid evidence in accordance with procedural law applicable in Indonesia. Consequently, emails, recorded chat files, and various other electronic documents may be used as admissible evidence.

Law No. 30 of 2002 explicitly grants the Corruption Eradication Commission (KPK) the authority to conduct interception and record communications for the purpose of conducting inquiry and investigation into corruption crimes. The KPK is authorized to use the results of interception as legally valid evidence in the investigation and prosecution of corruption cases in Indonesia. Technological advancements have broadened the types and forms of evidence. The KPK has collected and analyzed digital data such as digital recordings, emails, electronic banking transaction data, metadata, and electronic documents to prove corruption cases.

The KPK has used various forms of electronic evidence in the investigation and prosecution of corruption cases. The KPK has utilized audio and video recordings as evidence, such as recorded conversations between suspects and other parties. Electronic evidence in the form of CCTV recordings represents one of the most recent and significant types of evidence contributing to the clarity and efficiency of proving criminal acts, providing substantial assistance in illustrating a suspect's actions, thereby reducing unnecessary complexity during court proceedings (Rirynsusanti et.al, 2025). One of the functions of CCTV is to serve as a primary indicator when an incident occurs in the absence of eyewitnesses.

Therefore, CCTV is frequently presented as electronic evidence in criminal trials. CCTV, or closed-circuit television, consists of cameras connected to monitoring screens and is commonly used as a security device to monitor a specific location . CCTV

recordings can be submitted as electronic evidence because videos or images recorded by CCTV fall under the category of electronic information and/or electronic documents. Following the issuance of Constitutional Court Decision No. 20/PUU-XIV/2016 (hereinafter referred to as the 2016 Constitutional Court Decision), the role of CCTV evidence was subsequently limited to valid electronic circumstantial evidence.

The Corruption Eradication Commission employs Digital Forensics to analyze digital evidence and prove corruption cases. Digital forensics involves the forensic examination of investigative data found on digital devices such as computers and mobile phones. From a legal perspective, digital forensics plays a pivotal role in producing valid digital evidence that is admissible in court. Digital forensics is highly instrumental in verifying the authenticity of evidence in criminal cases (including corruption cases). For example, if the KPK obtains evidence in the form of intercepted communications, an expert in Audio Forensics will verify the authenticity of the recording. Similarly, WhatsApp conversations will be examined by a Mobile Forensics expert.

Digital forensics is a branch of forensic science focusing on the collection, analysis, and preservation of digital data for investigative purposes. One of its essential functions is to provide evidence that is legally admissible in court. Elements of digital forensic investigations include identifying, collecting, and analyzing data from various digital sources or devices, both through physical and non-physical communication channels, as well as from data storage media deemed relevant for presentation in court as supporting evidence in criminal proceedings (Amsori, 2024).

In corruption cases in the digital era, evidence often appears in electronic form, such as video recordings and digital communications. Computer metadata, data about data describes and provides additional key facts about documents, videos, photographs, or emails that are not visible to the naked eye. Metadata, which records information such as the date, time, and location of file creation, can be critical for reconstructing events. By analyzing metadata, the KPK can uncover the digital footprint of perpetrators, including information concealed from ordinary observation.

Commonly used forms of computer metadata include:

1. Files

Creation date, deletion date, author, and editing history.

2. Software Applications

Installation and uninstallation dates, frequency of use, and timestamps of use.

3. Browsing Metadata

Web search history, webpage titles and URLs, browser used, and visit timestamps.

Digital evidence encompasses various types of information stored on digital devices. Forensic experts are capable of recovering computer metadata evidence, including data that has been deleted or concealed, regardless of the condition of the computer or mobile phone. For example, forensic investigators search for indications of tampering, such as attempts to alter or destroy evidence. The Corruption Eradication Commission (KPK) employs digital forensics, including metadata analysis, to examine digital evidence in corruption cases. Digital forensics is essential for verifying the authenticity and validity of electronic evidence, such as video recordings or other electronic data by examining metadata and hash values to ensure that no manipulation has occurred.

The entire digital forensic process as outlined in ISO 27037 comprises four stages: identification of evidence at the crime scene, collection of data from discovered electronic devices, acquisition of electronic devices, and preservation of the evidence. The electronic evidence is subsequently strengthened through expert testimony from technical and professional specialists.

The Corruption Eradication Commission (KPK) has analyzed financial transaction data to trace the flow of funds and substantiate corruption cases. KPK uses financial transaction analysis to trace suspicious financial flows, often in cooperation with the Indonesian Financial Transaction Reports and Analysis Center (PPATK). PPATK is an institution specifically tasked with analyzing suspicious financial transaction reports to prevent and combat money laundering. KPK utilizes PPATK's data and analyses to support corruption investigations. The objective is to trace fund flows, identify the sources and destinations of illicit money, and gather strong evidence for corruption cases. This analysis serves as a key tool in uncovering corruption and money laundering crimes.

The Corruption Eradication Commission (KPK) has also employed Artificial Intelligence (AI) to uncover corruption-related crimes. Advances in technology have enabled perpetrators to use cyberspace platforms, data systems, and algorithms to commit corrupt acts. KPK has transformed its approach to meet these new challenges by adopting AI as a strategic instrument in the prevention and enforcement of corruption. AI is set to become a primary catalyst for the KPK's three core mandates: prevention, enforcement, and education. From detecting corruption patterns to enhancing public transparency, AI strengthens Indonesia's anti-corruption framework.

According to official information from the KPK, the Deputy for Information and Data, Eko Marjono, stated that AI will be applied for corruption risk detection, analysis of suspicious transactions, and data-driven enforcement support. Various AI tools, such as Microsoft Copilot, Gamma, and Sectors.app are used to improve work efficiency and enhance data analysis capabilities within the KPK. Artificial Intelligence is a computer-based system capable of performing tasks that normally require human intelligence. AI makes decisions by analyzing and utilizing data within the system, involving processes such as learning, reasoning, and self-correction (Lubis, 2021).

Electronic evidence can provide critical and in-depth information to reveal the truth and ensure justice in judicial processes. Electronic evidence can serve as accurate and trustworthy evidence in court, often possessing high integrity and being difficult to manipulate or alter. Additionally, electronic evidence broadens the scope of available evidence, such as electronic data, audio or video recordings and enhances the use of evidence in criminal cases. For example, electronic evidence may include records of electronic communications, CCTV recordings, financial transaction data, or relevant digital traces.

2.2 The Effectiveness of Electronic Evidence in Proving Corruption Crimes

Electronic evidence has emerged as a legal response to developments in both technology and information systems. The law has adapted its regulatory framework to accommodate the use of electronic evidence within judicial proceedings. Legal provisions governing electronic evidence aim to enhance the fairness and efficiency of the justice system. One of the primary challenges in utilizing electronic evidence is ensuring its authenticity, validity, and integrity. Therefore, regulations concerning electronic evidence are intended to establish the standards and procedures required for such evidence to be admissible and properly considered by the court. These include requirements relating to authenticity, integrity, and lawful methods of collection and presentation.

Procedural law, as formal law, has not yet fully accommodated electronic documents as evidence. Although electronic evidence is not explicitly regulated in the Indonesian Criminal Procedure Code (KUHP), several newer statutes explicitly recognize and legitimize the use of electronic evidence, such as Law No. 30 of 2002 on the Corruption Eradication Commission and Law No. 11 of 2008 on Electronic

Information and Transactions, which may serve as the legal basis for declaring electronic evidence admissible in court.

When dealing with criminal acts regulated under these special statutes, electronic evidence may be used as legally valid evidence during trial. Even though KUHAP does not expressly provide for electronic evidence, the principle of *lex specialis derogat legi generali* applies, meaning that special laws override general laws such as KUHAP. Consequently, the provisions in such special statutes may lawfully serve as the basis for recognizing electronic evidence as admissible.

Furthermore, ensuring integrity in the use of electronic evidence requires expertise capable of verifying the authenticity of electronic data. Thus, the expansion of evidentiary types, namely through the use of electronic evidence has become a necessary solution in strengthening law enforcement. In this context, digital forensics as a scientific method plays a crucial role in the evidentiary process of criminal cases involving electronic evidence.

The Constitutional Court of Indonesia, through Decision No. 20/PUU-XVI/2016, established legal standards for the use of electronic evidence. The Court held that electronic evidence (information and/or electronic documents), including the results of interception, may be regarded as valid evidence, provided that it is lawfully obtained and conducted for the purpose of law enforcement upon the request of the police, the prosecutor's office, and/or other legally mandated law enforcement agencies. If electronic evidence is obtained unlawfully, judges must disregard it and treat it as having no evidentiary value in court.

status of electronic evidence is of significant importance in judicial proceedings, as electronic information and/or electronic documents and/or their printouts constitute legally valid evidence extending the types of evidence recognized under Indonesian procedural law. This validity, however, is conditioned upon the use of an electronic system compliant with Law No. 19 of 2016 amending Law No. 11 of 2008 on Electronic Information and Transactions (Asimah, 2020).

Under Indonesian procedural rules, electronic evidence must be subject to testing to determine its admissibility, similar to other forms of evidence. This testing includes formal and material requirements, which vary depending on whether the electronic evidence is submitted in its original form or as a printout.

The material requirements for electronic evidence are provided in Article 5 paragraph (3) of the ITE Law, which states that electronic information and documents are

legally valid if processed through an electronic system in accordance with the provisions of the ITE Law. The formal requirements are stipulated in Article 5 paragraph (4) and Article 43 of the ITE Law, as follows:

1. Electronic information or documents do not apply to:
 - a. Letters which, under statutory requirements, must be produced in written form.
 - b. Letters and their documents which under statutory requirements must be produced as notarial deeds or deeds issued by an authorized official.
2. Searches or seizures of an electronic system must be conducted with the authorization of the head of the local district court.
3. Searches or seizures of an electronic system must be carried out while safeguarding the continuity of public services.

Article 6 of the ITE Law provides that electronic documents shall be deemed valid insofar as the information contained therein can be accessed, displayed, guaranteed in its integrity, and accounted for in explaining a particular legal state of affairs.

Referring to Article 5 paragraphs (3) and (4) in conjunction with Article 6 of Law No. 11 of 2008, including their explanatory provisions, electronic evidence is considered legally valid for proving criminal acts so long as the information contained therein can be accessed, displayed, its integrity is ensured (i.e., free from any alteration), and it can be legally accounted for.

3. CONCLUSION

Article 26A of Law No. 20 of 2001 on the Eradication of Corruption Crimes designates electronic evidence as an extension of legally admissible evidence for proving corruption offenses. Pursuant to the mandate of the Corruption Eradication Commission Law, specifically Article 12 paragraph (1) of Law No. 30 of 2002, the KPK is granted the authority to conduct interception and record communications occurring between perpetrators of corruption and other individuals involved in corrupt acts.

The Corruption Eradication Commission (KPK) has utilized electronic evidence in the investigation and prosecution of corruption cases, including the collection and analysis of various forms of digital data such as digital recordings, emails, electronic banking transaction data, and metadata. KPK employs digital forensics to analyze digital evidence and substantiate corruption cases. Additionally, the KPK conducts financial transaction analysis

to trace the flow of funds and prove corruption offenses. The KPK has also adopted artificial intelligence (AI) to support its investigative and analytical processes.

Electronic evidence may be used as legally valid evidence in court. Electronic evidence constitutes a legitimate evidentiary instrument that significantly facilitates the adjudication of criminal cases. Such evidence can be used as material for proof, thereby enabling judges to form a conviction regarding the truth of the criminal act (in this context, corruption) committed by the defendant. However, this validity is conditional upon the requirement that the electronic evidence, whether in the form of electronic information and/or electronic documents is processed through an electronic system that complies with the applicable statutory provisions, so that the evidence may be declared admissible in court.

REFERENCES

Books

- Amalia Syauket, Dwi Seno Wijanarko, 2024, Buku Ajar Tindak Pidana Korupsi, Malang, PT Literasi Nusantara Abadi Grup
- Elwi Danil, 2012, Korupsi, Konsep, Tindak Pidana dan Pemberantasannya, Jakarta, RajaGrafindo Persada
- Hari Sasongko dan Lili Rosita, 2003, Hukum Pembuktian dalam Perkara Pidana untuk Mahasiswa dan Praktisi, Bandung, Mandar Maju
- Moeljatno, 1995, Azas-Azas Hukum Pidana, Jakarta, Bina Aksara
- M Sobron Yamin Lubis, 2021, Implementasi Artificial Intellegence Pada System Manufactur Terpadu, Semnasterk, UISU

Regulations

- Law of the Republic of Indonesia Number 20 of 2001 concerning the Amendment to Law Number 31 of 1999 on the Eradication of Corruption Crimes
- Law Number 11 of 2008 on Electronic Information and Transactions
- Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions
- Law Number 19 of 2019 concerning the Second Amendment to Law Number 30 of 2002 on the Corruption Eradication Commission
- Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions

Journals

- Dewi Asimah, Menjawab Kendala Pembuktian Dalam Penerapan Alat Bukti Elektronik, Jurnal Hukum Peratun Vol 3 No 2, Agustus 2020
- Daniel David julio lakada, Debby Telly Antouw, Grace Yurico Bawole, Perkembangan Pengaturan Alat Bukti Elektronik Dalam Hukum Acara Pidana (Kajian Hukum Tentang Cybercrime), Jurnal Fakultas Hukum, UNSRAT, Lex crimen Vol.12.No 4,2024

Hasnawati, Mohammad Safrin, Kedudukan alat bukti Elektronik Dalam Pembuktian Tindak Pidana, Al Manhaj Jurnal Hukum dan Pranata Sosial Islam, Vol 5, No 2, 2023,

Rirynsusanti Muhammad, Syawal Abdul Adjid, Amriyanto, Penggunaan Alat bukti elektronik Dalam Konteks Penyadapan Menurut Peraturan Tindak Pidana Korupsi, Legal Spirit Volume 9 (2), 2025

Steve Jelly Walintukan, dientje Rumimpunu, Rudy R Watulingas Akibat Hukum Pelaku Penyadapan Ilegal (Intersepsi) Menurut Undang-Undang Telekomunikasi Serta Undang-Undang Informasi dan Transaksi Elektronik, Lex Crimen. XI, No 1, Jan. 2022

Wardhana Ard Syaputra, Muhammad Halley Yudhistira, Pengaruh Operasi Tangkap Tangan (ott) Terhadap Pelaporan Dugaan Tindak Pidana Korupsi Oleh Masyarakat (Studi Kasus KPK), Jurnal Kebijakan Ekonomi, vol 18, No 1, 2023

Internet

Dandi Athallah, Tindak Pidana Korupsi di Era digital, <https://www.kompasiana.com/dandiathallah//677e78bdc925c42d642c5462/tindak-pidana-korupsi-di-era-digital>

Digital Forensik Adalah Mengungkap Jejak Digital di Era Siber, <https://msf.telkomuniversity.ac.id/digital-forensik-adalah-mengungkap-jejak-digital-di-era-siber/>

<https://www.hukumonline.com/berita/a/mempertanyakan-bukti-elektronik-sebagai-alat-bukti-dalam-kasus-pidana-lt667b57ba9f459/>

Junaedi Seto Saputro, Korupsi Menghancurkan Harapan Kita Bersama, <https://www.djkn.kemenkeu.go.id/kanwil-rsk/baca-artikel/17406/Korupsi-Menghancurkan-Harapan-Kita-Bersama.html>

KPK Gelar Lokakarya Strategi Penyajian Alat Bukti Elektronik di Hakordia 2024, <https://www.kpk.go.id/id/ruang-informasi/berita/kpk-gelar-lokakarya-strategi-penyajian-alat-bukti-elektronik-di-hakordia-2024>

Metadata Komputer, https://www.howelawfirm.com.translate.goog/e-discovery-and-forensic/computer-evidence/computermetadata/?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=sge#:~:text=Commonly%20used%20computer%20metadata%20evidence,used%2C%20and%20time%20on%20websites

Melangkah Era Baru: KPK Manfaatkan AI Guna Berantas Korupsi di Ruang Digital, <https://www.kpk.go.id/id/ruang-informasi/berita/melangkah-ke-era-baru-kpk-manfaatkan-ai-guna-berantas-korupsi-di-ruang-digital>,

Nafiatul Munawaroh, Prosedur Meminta Rekaman CCTV, Prosedur Meminta Rekaman CCTV, <https://www.hukumonline.com/klinik/a/prosedur-meminta-rekaman-cctv-lt65fd511f493db/>

Saufa Ata Taqiyya, Syarat dan Kekuatan Hukum Alat Bukti Elektronik, www.hukumonline.com/klinik/a/syarat-dan-kekuatan-hukum-alat-bukti-elektronik-cl5461/#_ftn3

Willa Wahyuni, Mengenal Operasi Tangkap Tangan KPK,
[https://www.hukumonline.com/berita/
a/mengenal-operasi-tangkap-tangan-kpk-lt626ac7a171949/?page=1](https://www.hukumonline.com/berita/a/mengenal-operasi-tangkap-tangan-kpk-lt626ac7a171949/?page=1)